

# DEPARTMENT OF MENTAL HEALTH AND DEVELOPMENTAL DISABILITIES

## POLICIES AND PROCEDURES

*Subject:*  
**USES AND DISCLOSURES OF PHI  
TO BUSINESS ASSOCIATES  
UNDER HIPAA**

Effective Date:  
6/21/04

Policy Number:  
HIPAA 04-3

Review Date:  
5/10/06  
Revision Date:  
6/16/06

Entity responsible:  
Office of  
Legal Counsel

### 1. **Purpose:**

The purpose of this policy is to set guidelines the Department of Mental Health and Developmental Disabilities (DMHDD) must follow in sharing protected health information (PHI) with any business or agency with which the DMHDD contracts to provide services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, requires that when a covered entity such as DMHDD enters into a service contract with a business or agency, the DMHDD must have a business associate agreement (BAA) with that business or agency.

### 2. **Policy:**

- 2.1 The DMHDD and the Regional Mental Health Institutes (RMHIs) may disclose PHI to a business associate and may allow the business associate to create or receive PHI on its behalf, if the DMHDD/RMHI obtains assurances that the business associate will appropriately safeguard the information as required by HIPAA. The assurances required by HIPAA must be included in the terms of the contract with the business associate or other written agreement between the DMHDD/RMHI and the business associate.
- 2.2 The BAA between the DMHDD and the business associate must establish the permitted and required uses and disclosures of PHI by the business associate. The terms of the BAA may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of HIPAA if done by the DMHDD.
- 2.3 The terms of the BAA may permit the business associate to use and disclose PHI for the proper management and administration of the business associate and provide data aggregation services relating to the health care operations of the DMHDD/RMHI, provided that the business associate will:

- 2.3.1 Not use or further disclose PHI other than as permitted or required by the contract or as required by law;
  - 2.3.2 Use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the contract/agreement;
  - 2.3.3 Report to the DMHDD/RMHI any use or disclosure of PHI not provided for by the contract/agreement of which it becomes aware;
  - 2.3.4 Ensure that any agents of the business associate, including subcontractors, to whom the business associate provides PHI received from, created by, or received by, the business associate on behalf of the DMHDD/RMHI, are held to the same restrictions and conditions that apply to the business associate with respect to such information;
  - 2.3.5 Make available PHI to the individual/service recipient to inspect and copy, except to the extent that access may be denied pursuant to Tenn. Code Ann. § 33-3-112;
  - 2.3.6 Make available PHI for amendment by the covered entity and incorporate any amendments to PHI;
  - 2.3.7 Make available the information required to provide an accounting of disclosures;
  - 2.3.8 Make its internal practices, books, and records relating to the use and disclosure of PHI received from, created by, or received by, the business associate on behalf of the DMHDD/RMHI, available to the Secretary of the United States Department of Health and Human Services, if requested, for purposes of determining the DMHDD's compliance with HIPAA; and
  - 2.3.9 At the termination of the contract, return or destroy all PHI, received from, created by, or received by, the business associate on behalf of the DMHDD/RMHI, that the business associate maintains in any form and retain no copies of such information. If return or destruction is not feasible, the business associate must limit further uses and disclosures to those purposes that make the return or destruction of the information unfeasible.
- 2.4 If the DMHDD discovers a material breach pattern of practice, or violation of a contract by a business associate, the business associate must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, the DMHDD must terminate the contract with the business associate. If termination is not feasible, the DMHDD must report the problem to the Department of Health and Human

Services Office for Civil Rights pursuant to 45 C.F.R. § 164.504(e)(1). Failure to take these steps will put the DMHDD out of compliance with the Privacy Rule.

- 2.5 Before PHI may be disclosed to a business associate of an RMHI, the RMHI Privacy Officer must confirm with the Central Office Privacy Officer that a BAA has been executed between the business associate and the DMHDD. If a BAA has not been executed, PHI may not be disclosed to the business associate unless and until such an agreement has been completed.
- 2.6 The DMHDD/RMHI is not required to enter into a BAA with a health care provider in order to disclose to the health care provider PHI which is related to the treatment of an individual.
- 2.7 The Central Office Privacy Officer or designee must ensure that a BAA file is maintained at the Central Office, which must contain originals of all BAAs executed between the DMHDD and its business associates. All BAAs must be kept for six (6) years after the BAA is no longer in effect.

### **3. Procedure/Responsibility:**

- 3.1 The Central Office Privacy Officer/designee must ensure that every service contract contains a HIPAA compliance clause that provides for the execution of a BAA.
- 3.2 The Central Office Privacy Officer must ensure that BAAs are developed as required by HIPAA regulations for business associates of the DMHDD and the RMHIs.
- 3.3 When a Central Office or RMHI employee receives a request for PHI from a business associate to use for purposes other than treatment, payment or operations, s/he must check with the Central Office Privacy Officer to ensure that a BAA is on file.
- 3.4 The Central Office/RMHI HIPAA Privacy Officer must check the BAA files to verify who is requesting PHI and whether there is valid authorization for the disclosure.

### **4. Definitions:**

Business Associate: A person, business, agency, or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI), on behalf of, or provides services to, the DMHDD. A member of the DMHDD's

workforce, whether s/he is an employee or volunteer, and who is under the direct supervision or control of the DMHDD, is not a business associate.

Privacy Rule: "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information, promulgated by the Department of Health and Human Services (HHS), and found at 45 C.F.R. §§ 160 and 164, Subparts A and E. The Privacy Rule creates national standards and provides the first comprehensive federal protection for individuals' medical records and other personal health information.

Protected Health Information (PHI): "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 164.501, limited to the information created or received by business associate from or on behalf of the DMHDD. It includes, but is not limited to, medical records, and treatment and billing information.

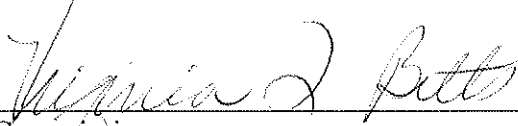
Required By Law: "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.501.

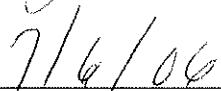
5. **Other Considerations:**

**Authority:**

Health Information Portability and Accountability Act of 1996, Public Law 104-191; HIPAA Regulations 45 C.F.R. §§ 160 and 164; 45 C.F.R. § 160.103; 45 C.F.R. §§ 164.501; 164.502(e)(1), (e)(2), and (g); 45 C.F.R. § 164.504; Tenn. Code Ann. §§ 33-1-303; 33-3-112.

Approved:

  
\_\_\_\_\_  
Commissioner

  
\_\_\_\_\_  
Date